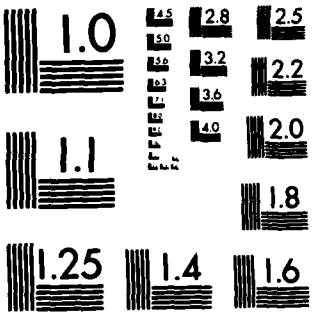
AD-A170 814 GORDIAN SYSTEMS ACCESS KEY(U) NATIONAL COMPUTER SECURITY CENTER FORT GEORGE G MEAD MD P HAGER ET AL. 07 APR 86 CSC-EPL-86/001 1/1

UNCLASSIFIED F/G 9/2 NL

END
DATE FILMED
9 86



SECURITY CLASSIFICATION OF THIS PAGE

AD-A170 814

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT: PUBLIC RELEASE - DISTRIBUTION UNLIMITED
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S): CSC-EPL-86/001	5. MONITORING ORGANIZATION REPORT NUMBER(S): S-228-218
6a. NAME OF PERFORMING ORGANIZATION: NATIONAL COMPUTER SECURITY CENTER; 6b. OFFICE SYMBOL (If applicable): C12	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code): 9800 Savage Road, Fort George G. Meade, MD 20755-6000	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION; 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS: PROGRAM ELEMENT NO; PROJECT NO.; TASK NO; WORK UNIT NO
11. TITLE (Include Security Classification): Final Evaluation Report of Gordian Access Key	
12. PERSONAL AUTHOR(S): HAGER, PAUL & BURNEY, CARL	
13a. TYPE OF REPORT: FINAL; 13b. TIME COVERED: FROM _____ TO _____	14. DATE OF REPORT (Yr., Mo., Day): 86/04/07; 15. PAGE COUNT: 14
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	Trusted Computer System Evaluation Criteria Gordian Systems Access Key EPL, NCSC, Access Key

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The Gordian Systems Access Key product was evaluated against the authentication requirements specified by the DoD Trusted Computer System Evaluation Criteria dated 15 August 1983. The Access Key system was found to satisfy some, but not all, of the user authentication requirements. The Access Key system is a user authentication mechanism for use with the computer systems which either lack a user authentication capability or require additional authentication assurance. The Access Key product is a "challenge/response" device. A hand-held encryption device (the Access Key) is used to read and decipher an encrypted flashing pattern from the terminal screen. The Access Key returns a password which allows the user to gain access to the host computer system.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT: UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☒ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION: UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL: MARIO TINTO, Chief, C12	22b. TELEPHONE NUMBER (Include Area Code): (301) 859-4458; 22c. OFFICE SYMBOL: C12

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE

FOREWORD

This publication, Final Report of the Gordian Systems Access Key Component Evaluation, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center". The purpose of this report is to document the results of a component evaluation of the Gordian Systems Access Key user authentication system (Release Version A.00).

FINAL REPORT
OF THE
GORDIAN SYSTEMS ACCESS KEY COMPONENT EVALUATION

TABLE OF CONTENTS

EVALUATION TEAM MEMBERS

Carl L. Burney
Paul R. Hager

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

EXECUTIVE SUMMARY

The Gordian Systems Access Key product is intended to serve as a user authentication mechanism for use on a wide range of host architectures. Since the Gordian Systems Access Key is a security component rather than a complete computer system, it was not evaluated against an entire class in the Department of Defense Trusted Computer System Evaluation Criteria, hereafter referred to as the "Criteria". Rather, it was assessed as to how well it performed user authentication.

The evaluation team has determined that the Access Key system is a useful and effective user authentication mechanism. The Access Key system can provide user authentication for computer security designs lacking such a feature or, by using it in conjunction with an existing authentication mechanism, can enhance authentication assurance. Once operational, the product constitutes a reliable authentication device which satisfies vendor claims regarding its user authentication capabilities (i.e., as described in the Gordian Systems' Access Management brochure, August 1985). Vendor claims, for the most part, refer to only one of the Criteria's requirements for user authentication, the capability to uniquely identify each system user. The Gordian Systems Access Key product is able to uniquely identify each user, but it does not provide protection for its authentication data (the second requirement for user authentication). The host's security system is responsible for restricting access to this host-resident security database.

The implementation of the product onto an ADP system requires a thorough understanding of the host system, the application language, and the security system currently in use by the host. Some familiarization with encryption concepts would be useful when reviewing the source code for logic flow. The product documentation clearly states that such technical expertise is expected of the implementor(s).

It is important to note that the functional integrity of the Access Key system's software and security database, both of which reside on the host system, depends upon the degree of protection provided them by the host's security system. It is for this reason that the Access Key system is intended for integration with an existing security package. Should the Access Key software and security database not be protected from unauthorized access and alteration, little trust could be placed in the Access Key system's operational reliability.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center (DoDCSC) was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September of 1984, the National Security Decision Directive 145 (NSDD-145) expanded these responsibilities to include all federal government agencies. At that time, the DoDCSC became known as the National Computer Security Center (NCSC).

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems, that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry and government developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements into the systems acquisition process.

The NCSC Component Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Component Evaluation Program.

The goal of the NCSC's Component Evaluation Program is to provide computer installation managers with information on components that would be helpful in providing immediate computer security improvements in existing installations.

Components considered in the program are special-purpose products which can be added to existing computer systems to increase some aspect of security and that have the potential of meeting the needs of government departments and agencies. For the most part, the scope of a component evaluation is limited to consideration of the component itself, and does not address or attempt to rate the overall security of the processing environment or computer system on which the component may be

implemented. To promote consistency in evaluations, and where appropriate, an attempt is made to assess a component's security-relevant performance in light of applicable standards and features outlined in the Criteria. In addition, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be made available to the public by placing it on the Evaluated Product's List (EPL).

The final evaluation report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT DESCRIPTION

Access Key Overview

The Gordian Access Key system is a user authentication mechanism intended for implementation on ADP systems which either lack a user authentication capability or require additional authentication assurance. The Access Key [illegible]s a Challenge/Response device. It confronts the user with a visual "challenge" and waits for the user to enter the expected "response", a six-character password generated by the hand-held Access Key.

The product makes use of data encryption when forming and validating the user password. Although the encryption algorithm itself is somewhat involved, use of the Access Key device is straight-forward. Prior to beginning the authentication process, the user must first log onto the host system. After the user has entered his personal ID, the Access Key protection program is invoked. The program, which resides on the host system, flashes a graphic pattern on the terminal screen. The user holds the domino-sized Access Key device to the screen and allows it to "read" the data represented by this flashing pattern. The Access Key device encrypts this data with seed information stored within its own memory cells. This encrypted six-character password is then presented on the Access Key's LCD display. The user enters this password to the host-resident protection program. The protection program verifies the correctness of the password before granting the user access to the host system.

Access Key Features

The Access Key is designed to serve as a hardware-independent, password-generating device which, in concert with host-resident software, provides the facility for controlling access to a specific computer system, network, data unit, or program. Its use as a component is for integration with an existing security system which provides audit and object access control functions. A significant feature of this authentication system is that one-time passwords are generated with each use of the Access Key.

The Gordian Access Key System consists of:

- a host-resident protection program
- hand-held Access Key devices (one per user)
- the "Key Cutter"

The host-resident protection program has two primary functions. It is responsible for forming and displaying a

pseudo-random number to the Access Key in the form of a graphic display (stimulus) on the terminal screen. It then must verify that the password entered by the user is the correct response for that specific user log-on ID.

The hand-held Access Key device is self-contained, battery-powered, and relatively small - about the size of a domino. It uses four optical sensors to read a flashing stimulus from the terminal screen. With the use of encryption routines, it converts the host-generated stimulus (i.e., a bit representation of the pseudo-random number) to a six-character password. This password is displayed on the Access Key's small LCD screen. The password is, in turn, used by the user to gain access to the host system. Each system user is issued a personalized Access Key device. Each Access Key device contains unique encryption/seed information.

As stated earlier, the protection program is aware of the user's ID because user log-on is completed prior to invocation of the Access Key system. Using the user's log-on ID to generate the password contributes to the uniqueness of each Access Key device. To correctly decrypt the password, the host-resident protection program must use the same seed information as that stored in the Access Key. This is accomplished by referencing a database containing the user's ID and the necessary seed information. This security database must be developed and placed on the host system by the customer.

The Key Cutter device programs each Access Key with seed information specific to the customer and the individual system user. This seed information will be used during the Access Key's encryption of the password. Access Keys have two resettable limits, a time limit and a usage limit. These limits can be used to control either the time duration or the number of uses for which the hand-held Access Key device will remain valid.

There are implementation peculiarities of this product which should be noted. Because the Access Key system will be implemented on systems with different architectures, specific subroutines within the protection program need to be tailored to each customer's operating system and security design. As a result, of the thirteen subroutines comprising the protection program, the customer would be required to construct five. Each of these five routines are relatively short and their implementation straight-forward.

Source listings of the vendor-provided protection routines are available in the Pascal, PL/1, and C program languages. The vendor will assist the customer in integrating those customer-written subroutines with the vendor code.

A critical assumption of this authentication system is that each user will maintain possession of his own Access Key and will immediately report its loss so that the lost key can be voided on the security database. Any user possessing a valid Access Key device and the corresponding user ID can gain access to the host system. Without proper control over the Access Keys, assurance in the system's authentication capability is lost. One benefit of linking the authentication process to possession of a physical device is that it becomes rather obvious to the user when his authentication capability has been compromised (i.e., the Access Key has been lost). Another point of particular importance is that security against unauthorized access and alteration of the protection program and security database is dependent upon the degree of protection afforded to them by the host operating system's security design. This is very important because the Access Key system software can not protect itself, but, rather, relies upon the operating system's security design for protection.

DOCUMENTATION OVERVIEW

All of the technical information relating to the Access Key system was obtained either through discussion with its designers or by review of product documentation. The Access Key system documentation is primarily for those individuals responsible for implementing the product on the host system. It assumes that these technicians have a sound understanding of what factors must be considered when interfacing feature-specific software with the host's operating system, data structures, and security design. A brief description of the documentation referenced by the evaluation team is provided below.

Access Key System Overview

This document presents an overview of the Access Key system. It describes:

- the Access Key device and its use
- the Access Key algorithm
- the security database
- the development and implementation of the protection program
- the Key Cutter and its use

Although it does not contain details of the encryption algorithm and seed values, Gordian Systems considers this document to be company proprietary.

Access Key Product Description

This document provides a detailed description of the Access Key device. The document addresses these device characteristics:

- physical specifications
- internal components
- Key usage

This document serves as a technical supplement to the Access Key Product Description paper. This document is company proprietary.

OEM Development Guide

This document is intended for use by the customer's system programmers when implementing the Access Key protection

DOCUMENTATION OVERVIEW

All of the technical information relating to the Access Key system was obtained either through discussion with its designers or by review of product documentation. The Access Key system documentation is primarily for those individuals responsible for implementing the product on the host system. It assumes that these technicians have a sound understanding of what factors must be considered when interfacing feature-specific software with the host's operating system, data structures, and security design. A brief description of the documentation referenced by the evaluation team is provided below.

Access Key System Overview

This document presents an overview of the Access Key system. It describes:

- the Access Key device and its use
- the Access Key algorithm
- the security database
- the development and implementation of the protection program
- the Key Cutter and its use

Although it does not contain details of the encryption algorithm and seed values, Gordian Systems considers this document to be company proprietary.

Access Key Product Description

This document provides a detailed description of the Access Key device. The document addresses these device characteristics:

- physical specifications
- internal components
- Key usage

This document serves as a technical supplement to the Access Key Product Description paper. This document is company proprietary.

OEM Development Guide

This document is intended for use by the customer's system programmers when implementing the Access Key protection

program on the host computer. Its purpose is to provide the necessary program logic, application requirements, and interface description so as to allow for the correct integration of the Access Key product with the host ADP system. The document contains:

- a top-down perspective of the system's functions
- an overview of the security database
- a detailed description of the stimulus display
- an algorithmic review of the protection routines
- a description of Access Key programming and the corresponding information within the security database
- source code listings of the vendor-provided portion of the Access Key protection program

As with the previous system documents, the OEM Development Guide is company proprietary.

In addition to these technical documents, Gordian Systems does provide the customer with an information packet which describes operation of the Access Key from a user's perspective.

Although the available Access Key documentation contains detailed description of the product's composition and implementation, it does not address the security measures required of the host system. The host-resident Access Key software and security database must be protected from subversion. Since the product's integrity is dependent upon the correct operation of the host-resident protection program, it is recommended that the customer be clearly informed as to what steps should be taken to protect both the software and security data from improper alteration. Such information could be included in the OEM Development Guide.

PRODUCT FUNCTIONALITY

Test Procedures

As was stated in the Product Overview section of this report, the Gordian Access Key system does not arrive at the customer's site fully operational. The customer must provide five implementation-dependent software subroutines to complete the protection program. The customer must also use the Key Cutter device to initialize his user Access Keys. The vendor will do this Access Key initialization for the customer if so requested, but possession of the Key Cutter would be an advantage should the customer wish to initialize new Access Keys.

This brief review of the product's implementation process directly relates to the evaluation team's approach to testing the Access Key system. Since a Gordian Systems Access Key customer would first be required to complete the protection program software and integrate the product with the host system, a clearer and more complete analysis of the product would result if the evaluation team played the role of a customer and went through the entire process of product implementation. By doing so, the evaluation team gained both an understanding of the Access Key's functionality and insight into the implementation difficulties associated with this product.

The NCSC does not directly evaluate or comment upon the strengths or weaknesses of encryption algorithms. For this reason, testing of the product focused upon its ability to properly display the stimulus to the Access Key and discern the correctness of the entered password. There was no attempt on the part of the evaluation team to scrutinize or qualify the integrity of the Access Key's encryption algorithm.

Two Access Key systems were examined in this evaluation. The one system was developed and integrated by the evaluation team and the other was provided to the team by the vendor in the form of a fully-functional software package containing system documentation, Access Keys, and protection program source listings. Both Access Key systems were implemented on an IBM XT personal computer.

Changes to vendor-provided source code were required for the Access Key system assembled by the evaluation team. Specifically, the software responsible for flashing the graphic representation of the random number onto the terminal screen had to be slightly altered. This was largely due to the graphics capabilities of the host compiler. Modifications to a decryption subroutine were also required so as to accommodate a 16 rather than a 32-bit internal storage format. This was

necessary because the routine's calculations were predicated upon a 32-bit word field and the host system used for testing could not provide that capability.

Once the protection program and security database were implemented on the host system, the evaluation team traced each protection subroutine, line-by-line. By manually computing variable and argument values through each routine, snapshot values of these variables were compared against those provided by the protection program during actual execution. By this "Walk-Thru" type of software analysis, the evaluation team was able to ensure that each routine within the protection program executed precisely as stated in the system documentation.

The second Access Key system was sent to the evaluation team as a fully operational package. It had been developed by Gordian system designers for use by customers and so had been tailored for application on a minicomputer. As with the Access Key system implemented by the evaluation team, this source code was, again, carefully reviewed and snapshot values of significant variables were checked for correctness. Special attention was paid to the protection subroutines which decrypt the six-character password and compare the resulting bits to the bit stream comprising the original stimulus displayed on the terminal screen. The team's software testing of the product provided assurance as to the product's functional correctness in comparing the two bit-vectors. Although the test suite was relatively small, the evaluation team did attempt, without success, to gain access to the host system by using incorrect passwords.

Test Results

As was mentioned in the Test Procedures section of the report, technical difficulties encountered by the evaluation team during implementation of the Access Key system were largely due to the need to adapt vendor-supplied software to the specific host architecture and operating system (e.g., the 16 versus 32-bit internal format, and host software graphics capabilities)

Such software modifications were not necessary for the packaged Access Key system sent to the evaluation team by the vendor. In fact, this Access Key system contained special diagnostic software so as to assist the customer with program debugging during product implementation.

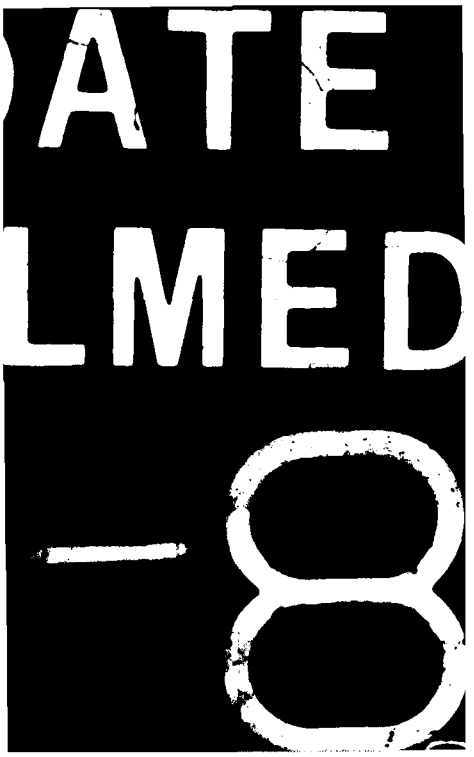
Gordian Systems realizes that in order to increase product reliability and facilitate its implementation, the amount of software development required of the customer should be minimized. Although software tailoring by the customer is being

reduced, the protection program will still require some customizing to the host environment. By introducing a new, hand-held, stimulus-generating device (the Keypad), Gordian designers have also taken steps to increase the reliability of the Access Key's reading of the visual stimulus.

In summation, the Gordian Access Key system does provide a useful and effective user authentication capability to host systems lacking such a feature or to computer security systems requiring additional user authentication. The product is able to uniquely identify each system user. However, it does not provide for the protection of the user authentication data stored on the host system.

As mentioned earlier in the report, the functional integrity of the protection software and security database is dependent upon the the degree of protection provided to them by the host's security system. It is for this reason that the Access Key product is well-suited for integration with an existing security package capable of controlling user access to its storage objects.

☆U.S. Government Printing Office: 1988—622-340/80316


ATE
LMED
8